



НЕКОММЕРЧЕСКОЕ ПАРТНЕРСТВО

НАЦИОНАЛЬНЫЙ СОВЕТ ФИНАНСОВОГО РЫНКА

101000, г. Москва, ул. Мясницкая, дом 42, стр. 3

телефон/факс : (499) 678 28 20

исх. *НСФР-02/1-478*

от *01.06.2018*

Директору Департамента
информационной безопасности
Банка России
Уварову В.А.

*О надзоре за соблюдением кредитными
организациями требований Федерального
закона от 31.12.2017 № 482-ФЗ в части
обработки персональных данных*

Уважаемый Вадим Александрович!

Настоящее обращение Национального совета финансового рынка обусловлено возникающими у кредитных организаций вопросами о порядке осуществления надзора за их деятельностью при применении положений Федерального закона от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Закон № 482-ФЗ) в частности обработки персональных данных.

В соответствии с пунктом 5.6 статьи 7 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», введенным Законом № 482-ФЗ, кредитная организация обязана после проведения идентификации при личном присутствии клиента – физического лица, являющегося гражданином Российской Федерации, с его согласия и на безвозмездной основе размещать или обновлять в электронной форме в единой системе идентификации и аутентификации сведения, необходимые для регистрации в ней клиента – физического лица, и сведения, предусмотренные абзацем вторым подпункта 1 пункта 1 статьи 7, а также в единой информационной системе персональных данных, обеспечивающей сбор, обработку, хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее – ЕБС), его биометрические персональные данные.

На сегодняшний день ряд элементов регуляторной базы по сбору и обработке соответствующих персональных данных продолжает находиться в стадии нормативной и технической доработки, в связи с чем для реализации предусмотренных Федеральным законом № 115-ФЗ требований по обработке биометрических персональных данных, а также проверке и передаче информации о степени их соответствия, необходимо будет провести комплекс дополнительных организационно-технологических мероприятий.

В соответствии с Информационным письмом Банка России от 28.06.2018 № ИН-03-13/40 «Об особенностях применения мер к банкам при совершении ими действий, предусмотренных пунктом 5.6 статьи 7 Федерального закона от 7 августа 2001 года N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"» все банки, соответствующие законодательно установленным критериям, обеспечивают принятие организационно-технических мер защиты информации от угроз безопасности, актуальных при обработке, включая сбор и

хранение, биометрических персональных данных, их проверке из числа установленных Банком России в соответствии с частью 14 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – перечень актуальных угроз Банка России), в части угроз нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных) при сборе биометрических персональных данных в банках, включая непосредственный сбор биометрических персональных данных и передачу собранных биометрических персональных данных между собственными внутренними структурными подразделениями банков.

Таким образом, кредитные организации в настоящее время самостоятельно принимают решения (в том числе о технических параметрах инфраструктуры для обработки персональных данных) в целях соблюдения требований Закона № 482-ФЗ, что, как представляется, создает для кредитных организаций определенные риски надзорного воздействия со стороны уполномоченных органов.

При этом согласно статье 4 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» полномочия по надзору за деятельностью кредитных организаций и банковских групп закреплены исключительно за Банком России.

В соответствии с пунктами 10 и 11 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (введена Законом № 482-ФЗ), контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», при обработке персональных данных в единой биометрической системе, за исключением контроля и надзора за выполнением кредитными организациями организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, а контроль и надзор за выполнением кредитными организациями организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы осуществляются Банком России.

В этой связи просим Департамент информационной безопасности Банка России подтвердить правомерность вывода о том, что единственным надзорным органом, имеющим полномочия на применение к кредитным организациям мер надзорного воздействия в случае несоблюдения ими положений Закона № 482-ФЗ, в том числе при обработке персональных данных в процессе сбора, обработки, размещения, проверки и обновления сведений, как при первичном размещении сведений о физических лицах в ЕСИА и ЕБС, так и при осуществлении дистанционной идентификации физических лиц с использованием ЕСИА и ЕБС, является Банк России.

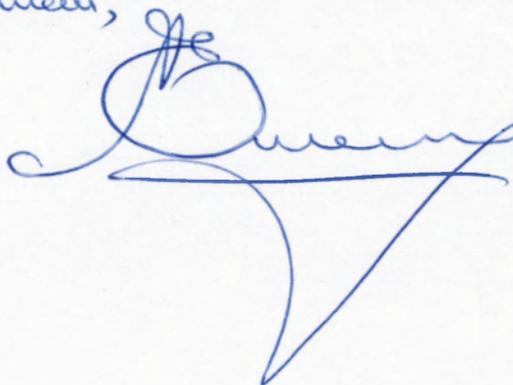
Дополнительно просим подтвердить, правомерность вывода о том, что при реализации мер защиты, предусмотренных перечнем актуальных угроз Банка России, не потребуется аттестация рабочих мест сотрудников банков, на которых выполняется непосредственный сбор биометрических персональных данных, а также аттестация сетей связи, используемых для передачи собранных биометрических персональных данных между собственными внутренними структурными подразделениями банков при условии применения сертифицированных программно-аппаратных средств и предусмотренных

действующим законодательством Российской Федерации процедур оценки корректности их встраивания.

НСФР выражает уверенность в дальнейшем плодотворном сотрудничестве с Департаментом информационной безопасности Банка России.

С уважением,

Председатель



А.В. Емелин